21世纪高等院校计算机网络工程专业规划教材

# 网络安全与信息保障

仇建平 编著

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

# 网络安全与信息保障

仇建平 编著

清华大学出版社
北京

## 内 容 简 介

本书全面介绍了网络安全与信息保障的基本框架，网络安全与信息保障的基本理论，以及网络安全与信息保障方面的管理、配置和维护，具有如下特点。

- 内容先进，结构新颖。书中吸收了国内最先进的新技术、新知识、新方法和国际通用准则，注重科学性、先进性、操作性。
- 注重实用的特色。坚持“实用、特色、规范”的原则，突出实用及素质能力培养，在内容安排上，通过大量案例将理论知识与实际应用有机结合。
- 资源配套。本书提供配套的电子教案，并有辅助的实验，内容包括学习指导、实验教学、练习测试和课程设计等。

本书可作为本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。



**图书在版编目(CIP)数据**

网络安全与信息保障/仇建平编著. —北京：清华大学出版社，2012.1
(21世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-26864-2

Ⅰ. ①网… Ⅱ. ①仇… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第211679号

**责任编辑**：高买花
**封面设计**：常雪影
**责任校对**：焦丽丽
**责任印制**：王静怡
**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
**印 装 者**：北京市密东印刷有限公司
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：18.5　　**字　　数**：448千字
**版　　次**：2012年1月第1版　　**印　　次**：2012年1月第1次印刷
**印　　数**：1～3000
**定　　价**：29.00元

产品编号：039858-01

# 前言

随着计算机网络技术的飞速发展，互联网已经深入到社会的各个方面，它对人们的工作方式、生活方式甚至思维方式都产生了巨大的影响，因此，可以说互联网已经成为现代人生活中不可缺少的一部分。

但是，人们在享受互联网所带来愉悦的同时，也不可避免地受到一系列网络及信息安全问题的困扰：网络上充斥虚假信息、非法信息，病毒日益猖狂，黑客攻击无孔不入等，这些都严重危及到个人、企事业单位乃至国家的信息安全。研究如何采取有效的方法来保护重要信息变得越来越有必要，本书便是在这样一个大背景下编撰而成的。

本书立足于当前网络安全与信息保障的具体实践，深刻而全面地反映了现代网络安全与信息保障的新理论、新方法、新成果。本书在内容的选择上注重学术性、实用性、创新性与可获得性，同时也综合考虑了不同学校和不同单位的教学实际，力求内容典型、精炼、新颖，具有代表性和可操作性。创造性地将网络安全与信息保障工具融进了传统教学中，充分揭示了网络安全与信息保障的新进展；系统而全面地介绍了常用的网络安全与信息保障理论；集中介绍了网络安全与信息保障实践，相关实验的介绍基本涵盖了网络安全与信息保障有关的内容；系统而全面地阐述了网络攻防的途径与方法，重点介绍了网络攻防的实例；系统而全面地总结了网络安全与信息保障的国内外进展。其中，网络攻防是国内相近专著和教材中所未包含的全新内容。

在全面总结当前国内外网络安全与信息保障和利用教材、专著、教学实践经验的基础上，提炼出基本适合于网络安全与信息保障教学、能力教育与培养的核心内容，在教学实践基础上增加了创新性的新内容，相关内容丰富了网络安全与信息保障理论，对于增强学生的相关能力，提高综合素质都有重要的意义。

因此，本书作为一本以信息安全为核心的教材，从实用和可获得性理论的角度出发专门介绍网络攻防的方法和技巧，这是国内对网络安全与信息保障课教学实践和教材使用上的大胆创新，对于全面提高信息管理、计算机科学与技术专业学生的信息素质和综合利用相关工具进行信息安全管理的能力、增强学生的信息安全意识和管理信息能力都有重要的现实意义和深远影响。

编　者

2011 年 9 月

# 目 录

# 第1章 网络安全与信息保障概述

本章首先讲述网络安全与信息保障的定义、内涵、目标等内容，通过这些概述性内容，使读者对网络安全与信息保障有一个大致的了解。

## 1.1 引　　言

20世纪40年代，随着计算机的出现，计算机安全问题也随之产生。随着计算机在社会各个领域的广泛应用和迅速普及，使人类社会步入信息化时代，以计算机为核心的安全、保密问题越来越突出。

20世纪70年代以来，在应用和普及的基础上，以计算机网络为主体的信息处理系统迅速发展，计算机应用也逐渐向网络化发展。网络化的信息系统是集通信、计算机和信息处理于一体的，是现代社会不可缺少的基础。计算机应用发展到网络阶段后，信息安全技术得到迅速发展，原有的计算机安全问题增加了许多新的内容。

同以前的计算机安全保密相比，计算机网络安全技术的问题要多得多，也复杂得多，涉及物理环境、硬件、软件、数据、传输、体系结构等各个方面。除了传统的安全保密理论、技术及单机的安全问题以外，计算机网络安全技术包括了计算机安全、通信安全、访问控制的安全，以及安全管理和法律制裁等内容，并逐渐形成独立的学科体系。

当今社会是一个信息化社会，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息化社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集于计算机中。但是这些信息系统都是依靠计算机网络接受和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息化社会的一个重要特征。随着网络的开放性、共享性及互联程度的扩大，特别是Internet的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，例如电子商务(Electronic Commerce)、电子现金(Electronic Cash)、数字货币(Digital Cash)、网络银行(Network Bank)等的兴起，以及各种专用网(如金融网等)的建设，使得安全问题显得越来越重要，因此对网络安全的研究成了现在计算机和通信界的一个热点。

简单地说，在网络环境中的安全是指一种能够识别和消除不安全因素的能力。安全的一般性定义也必须解决保护财产的需要，包括信息和物理设备(如计算机本身)。安全的想法也涉及适宜性和从属性概念。负责安全的任何一个人都必须决定谁在具体的设备上进行合适地操作，以及什么时候。当涉及公司安全的时候什么是适宜的，在公司与公司之间是不

同的，但是任何一个具有网络的公司都必需具有一个解决适宜性、从属性和物理安全问题的安全政策。

伴随着现代的、先进的复杂技术，例如局域网和广域网、Internet，安全的想法和实际操作已变得更加复杂。

计算机网络安全之所以重要，其主要原因在于以下几个方面。

(1) 计算机存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

(2) 随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂、系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑联结数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

(3) 人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转、不可替代的。

(4) 随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误和缺乏经验都会造成系统的安全功能不足。

(5) 计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、检验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄漏技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

(6) 从认识论的高度看，人们往往首先关注对系统的需要，然后才被动地从现象注意系统应用的安全问题。因此广泛存在着重应用轻安全、法律意识淡薄、计算机素质不高的普遍现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐藏的、潜在的、难以明确却又广泛存在的。

学习计算机网络安全技术的目的不是要把计算机系统武装到百分百安全，而是使之达到相当高的水平，使入侵者的非法行为变得极为困难、危险、耗资巨大，获得的价值远不及付出的代价高。

### 1.1.1 信息安全概述

信息是一种资产，就像其他重要的商业资产一样，它对一个组织来说是有价值的，因此需要妥善进行保护。信息安全保护信息免受多种威胁的攻击，保证业务连续性，将业务损失降至最少，同时最大限度地获得投资回报和利用商业机遇。信息存在的形式多种多样。它可以打印或写在纸上，以电子文档形式存储，通过邮寄或电子手段传播，以胶片形式显示或在交谈中表达出来。不管信息的形式如何，或通过什么手段进行共享或存储，都应加以妥善保护。

信息安全具有以下特征。

① 保密性：确保只有经过授权的人才能访问信息。

② 完整性：保护信息和信息的处理方法准确而完整。

③ 可用性：确保经过授权的用户在需要时可以访问信息并使用相关信息资产。

信息安全是通过实施一整套适当的控制措施实现的。控制措施包括策略、实践、步骤、

组织结构和软件功能。必须建立起一整套的控制措施，确保满足组织特定的安全目标。

### 1.1.2 对信息的安全需求的理解

信息和支持进程、系统以及网络都是重要的业务资产。为保证组织富有竞争力，保持现金流顺畅和组织赢利，以及遵纪守法和维护组织的良好商业形象，信息的保密性、完整性和可用性是至关重要的。

各个组织及其信息系统和网络所面临的安全威胁与日俱增，来源也日益广泛，包括利用计算机欺诈、窃取机密、恶意诋毁破坏等行为，以及火灾或水灾。危害的来源多种多样，如计算机病毒、计算机黑客行为、拒绝服务攻击等，这些行为呈蔓延之势、用意更加险恶，而且手段更加复杂。组织对信息系统和服务的依赖意味着自身更容易受到安全威胁的攻击。公共网络与专用网络的互联以及对信息资源的共享，增大了对访问进行控制的难度。分布式计算尽管十分流行，但降低了集中式专家级控制措施的有效性。很多信息系统在设计时，没有考虑到安全问题。通过技术手段获得安全保障十分有限，必须辅之以相应的管理手段和操作程序才能得到真正的安全保障。确定需要使用什么控制措施需要周密计划，并对细节问题加以注意。

作为信息安全管理的最基本要求，组织内所有的雇员都应参与信息安全管理。信息安全管理还需要供应商、客户或股东的参与。也需要参考来自组织之外的专家建议。

如果在制定安全需求规范和设计阶段时就考虑到了信息安全的控制措施，那么信息安全控制的成本会很低，并更有效率。

### 1.1.3 网络安全潜在威胁及不安全因素

**1. 网络安全潜在威胁**

计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；也有可能是外来黑客对网络系统资源的非法使用。

目前，归结起来网络安全所面临的主要潜在威胁有以下几方面。

(1) 信息泄密。主要表现为网络上的信息被窃听，这种仅窃听而不破坏网络中传输信息的网络侵犯者称为消极侵犯者。

(2) 信息被篡改。这就是纯粹的信息破坏，这样的网络侵犯者称为积极侵犯者。积极侵犯者截取网上的信息包，并对之进行更改使之失效，或者故意添加一些有利于自己的信息起到信息误导的作用。积极侵犯者的破坏作用最大。

(3) 传输非法信息流。用户可能允许自己同其他用户进行某些类型的通信，但禁止其他类型的通信，如允许电子邮件传输而禁止文件传送。

(4) 网络资源的错误使用。如果不合理地设定资源访问控制，一些资源有可能被偶然或故意地破坏。

(5) 非法使用网络资源。非法用户登录进入系统使用网络资源，造成资源的消耗，损害合法用户的利益。

(6) 计算机病毒已经成为威胁网络安全的最大威胁。

**2. 不安全因素**

由于网络所带来的诸多不安全因素使得网络使用者不得不采取相应的网络安全对策。为了堵塞安全漏洞和提供安全的通信服务，必须运用一定的技术来对网络进行安全建设，建立完善的法律、法规及完善管理制度，提高人们的安全意识，这已成为广大网络开发商和网络用户的共识。

依据网络与信息所面临的威胁可将网络及信息的不安全的因素归结为自然灾害和人为灾害、系统物理的故障、人为的无意失误、网络软件的缺陷、计算机病毒、法规与管理不健全。

(1) 自然灾害：包括水灾、火灾、地震、雷击、台风及其他自然现象造成的灾害。

(2) 人为灾害：包括战争、纵火、盗窃设备及其他影响到网络物理设备的犯罪等。

**注意**：自然灾害和人为灾害虽然发生的概率很小，但也不容忽视。

(3) 系统物理故障：包括硬件故障、软件故障、网络故障和设备环境故障等。

电子技术的发展使电子设备出现故障的概率在几十年里一降再降，许多设备在它们的使用期内根本不会出错。但是由于计算机和网络的电子设备往往极多，故障还是时有发生。由于器件老化、电源不稳、设备环境等很多问题使计算机或网络的部分设备暂时或永久失效。这些故障一般都具有突发的特点。

对付电子设备故障的方法是及时更换老化的设备，保证设备工作的环境，不要把计算机和网络的安全与稳定联系在某一台或几台设备上。另外还可以采用较为智能的方案，例如现在智能网络的发展，能使网络上出现故障的设备及时退出网络，其他设备或备份设备能及时弥补空缺，使用户感觉不到网络出现了问题。

软件故障一般要寻求软件供应商来解决，或者更换、升级软件。

(4) 人为的无意失误：包括程序设计错误、误操作、无意中损坏和无意中泄密等。如操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。这些失误有的可以靠加强管理来解决，有的则无法预测，甚至永远无法避免。限制个人对网络和信息的权限，防止权力的滥用，采取适当的监督措施有助于部分解决人为无意失误的问题。出现失误之后可以及时发现，及时补救也能大大减少损失。

## 1.2 网络安全与信息保障技术的发展

为了维护网络与信息系统的安全，单纯凭技术力量解决是不够的，还必须依靠政府和立法机构制定出完善的法律法规进行制约，给非法攻击者以威慑。只有全社会行动起来共同努力，才能从根本上治理高科技领域的犯罪行为，确保网络与信息的应用和发展。

在网络安全系统的法规和管理方面，我国起步较晚，目前还有很多不完善、不健全的地方，这给了某些不法分子可乘之机。但是政府和立法机构已经注意到了这个问题，立法工作正在迅速进行，而且打击力度是相当大的。各个公司、部门的管理者也逐步关心这个问题。随着安全意识的进一步提高，由于法规和管理不健全导致的安全威胁将逐渐减少。

### 1.2.1 网络安全体系结构

为了适应网络技术的发展，国际标准化组织(ISO)的计算机专业委员会根据开放系统

互联参考模型制定了一个网络安全体系结构模型。这个三维模型从比较全面的角度来考虑网络与信息的安全问题。

网络安全需求应该是全方位的、整体的。在 OSI 7 个层次的基础上，将安全体系划分为 4 个级别：网络级安全、系统级安全、应用级安全及企业级安全，而安全服务渗透到每一个层次，从尽量多的方面考虑问题，有利于减少安全漏洞和缺陷。

### 1.2.2 主要的安全服务

针对网络系统受到的威胁，OSI 安全体系结构提出了以下几类安全服务。

(1) 身份认证(Authentication)：这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务。这种服务防止冒充或重传以前的连接，即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的也可以是双向的。

(2) 访问控制(Access Control)：访问控制服务可以防止未经授权的用户非法使用系统资源。这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。

(3) 数据保密(Data Confidentiality)：数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。

(4) 数据完整性(Data Integrity)：这种服务用来防止非法实体对用户的主动攻击(对正在交换的数据进行修改、插入、使数据延时及丢失数据等)，以保证数据接收方收到的信息与发送方发送的信息完全一致。

(5) 不可否认性(Non-Repudiation)：这种服务有两种形式。第一种形式是源发证明，即某一层向上一层提供的服务，它用来确保数据是由合法实体发出的，它为上一层提供对数据源的对等实体进行鉴别，以防假冒；第二种形式是交付证明，用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。

(6) 审计管理(Auditing Management)：对用户和程序使用资源的情况进行记录和审查，可以及早发现入侵活动，以保证系统安全，并帮助查清事故原因。

(7) 可用性(Availability)：保证信息使用者都可得到相应授权的全部服务。

### 1.2.3 网络安全服务与网络层次关系

从网络的 7 个层次的角度来考虑安全问题，比较接近网络和应用系统的结构层次，便于充分全面地考虑具体实际的软件、硬件的安全。例如，拿到一个通信软件，可以从协议层次角度分析该软件从应用层到网络层的哪些层次上加了安全的保护，各层的安全性强度如何，哪一层上最容易受到攻击等。

由于 OSI 参考模型是一种层次结构，某种安全服务由某些层次支持更有效，而另外一些层次却不能支持。因此，存在一个安全服务与网络层次的配置问题，在这些层次之中，上一层的安全对下层的安全也有一定的依赖性，但与系统的层次不一样，各层的安全性可以是独立的。下层实现的安全对上层可以是透明的，也就是说上层感觉不到下层已经实现了安全。而下层不安全时，上层也可以独立实现安全。

### 1.2.4 网络安全标准

在完成关于一些安全基础的讨论后，下面介绍几种已存在的安全标准。

**1. ISO 7498-2**

安全体系结构文献定义了安全就是最小化资产和资源的漏洞。资源可以指任何事物；漏洞是指任何可以造成破坏系统或信息的弱点；威胁是指潜在的安全破坏。ISO 还进一步为威胁进行分类，例如，在前面介绍的不安全因素。ISO 7498-2 安全体系结构文献中还定义了几种安全服务。

ISO 7498-2 中描述的安全体系结构的 5 种安全服务项目是：鉴别、访问控制、数据保密、数据完整性和抗否认。

为了实现 5 种安全服务，制定了 8 种安全机制是：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务填充机制、路由控制机制和公正机制。

**2. 橘皮书**

目前广为流行的美国国防部开发的计算机安全标准——可信任计算机标准评价准则(Trusted Computer Standards Evaluation Criteria，TCSEC)，即网络安全橘皮书用来评价一个计算机系统的安全性。TCSEC 将计算机系统的可信任程度，即安全等级划分为 4 类 7 级，按安全程度从最低到最高的完全排序是 D、C1、C2、B1、B2、B3、A1。

### 1.2.5 安全策略的重要性

网络安全的一个最重要的任务就是制定一个安全策略。多数的用户都想用一个技术方案来解决每个问题，然而一个深思熟虑的安全规划，将帮助用户决定哪些需要保护，由谁来负责执行保护。

安全策略的目的是决定一个组织机构怎样来保护自己。一般来说，策略包括两个部分：总体的策略和具体的规则。总体的策略用于阐明公司安全政策的总体思想，而具体的规则用于说明什么活动是被允许的，什么活动是被禁止的。

**1. 制定组织机构的整体安全策略**

整体安全策略制定组织机构的战略性安全指导方针，并为实现这个方针分配必要的人力物力。一般是管理层的官员，如组织机构的领导者和高层领导人员来主持制定这种策略以建立该组织机构的计算机安全计划和其基本框架结构。

**2. 制定和系统相关的安全策略**

一般根据整体策略提出一个系统的具体保护措施。这种策略着重于某一具体的系统，更为详细。

安全策略的制定是为了保证信息的保密性、完整性和可用性，因此应具有普遍的指导意义。应该针对安全系统所面临的各种威胁，提出控制策略，并为系统的配置、管理和应用提供基本的框架。有了安全策略，系统才可能正常、有序地运行，也才可能更安全、合理地使用信息系统资源。有了安全策略，才可能更加高效、迅速地解决安全问题，使威胁造成的损失降为最小。制定安全策略的依据如下。

(1) 须对资源进行评估，包括硬件、软件、数据、文档等分出安全等级。

(2) 对可能的威胁进行分析，包括非授权访问、信息泄漏和内部缺陷等。

(3) 确定用户的权力和责任，包括账户管理、资源访问权限、口令应用及建立备份等。

(4) 明确系统管理员的权力和责任，包括物理安全、系统配置、账户设置及使用权限、口令管理、审计和监控等方面。

(5) 提出一般性的安全防护措施：存取控制、认证、密码技术、防火墙技术、操作系统安全、数据库系统安全、计算机病毒防护、审计和恢复等。

(6) 在安全维护方面，企业应注意当安全事件发生时应如何处理，因此应有完善的事故处理及事后处理的策略和制度。

## 1.3 信息安全管理的模型(SSE-CMM)

### 1.3.1 背景

系统安全工程能力成熟模型(Systems Security Engineering Capability Maturity Model，SSE-CMM)，描述了一个组织的安全工程过程必须包含的本质特征，这些特征是完善的安全工程保证。尽管 SSE-CMM 没有规定一个特定的过程和步骤，但是它汇集了工业界常见的实施方法。它覆盖了以下内容：

(1) 整个生命期：包括开发、运行、维护和终止。

(2) 整个组织：包括其中的管理、组织和工程活动。

(3) 与其他规范并行的相互作用：如系统、软件、硬件、人的因素、测试工程、系统管理、运行和维护等规范。

(4) 与其他机构的相互作用：包括获取、系统管理、认证、认可和评价机构。

在 SSE-CMM 描述中，提供了对所基于的原理、体系结构的全面描述；模型的高层综述；适当运用此模型的建议；包括在模型中的实施以及模型的属性描述。它还包括了开发该模型的需求。SSE-CMM 评定方法部分描述了针对 SSE-CMM 来评价一个组织的安全工程能力的过程和工具。

无论是顾客，还是供应商都对改进安全产品、系统和服务的开发感兴趣。安全工程领域已有一些被充分接受的原则，但目前仍缺少一个易于理解的评估安全工程实施的框架。SSE-CMM 正是这样一个框架，它为安全工程原则的应用提供了一个衡量和改进的途径。

必须强调安全工程是一个独特的科目，需要独特的知识、技能和过程来创建一个专用于安全工程的 CMM。这与安全工程将在系统工程方式下进行并不冲突。事实上，有明确定义和易于接受的活动可以使安全工程能够在各种情况下更有效地加以实施。

现代统计过程控制理论表明通过强调生产过程的高质量和在过程中组织实施的成熟性可以低成本地生产出高质量产品。对于安全系统和可信产品的开发，如果增加所需的成本和时间，就可保证更有效的过程。安全系统的运行与维护也依赖于与人员和技术相联系的过程。通过强调所使用过程的质量和蕴涵在这些过程中的组织实施的成熟性，可以更低成本地管理这些安全工程。

SSE-CMM 项目的目标是促进安全工程成为一个确定的、成熟的和可度量的科目。这个 SSE-CMM 和正在开发的评定方法，将带来以下益处：

(1) 通过区分投标者的能力级别和相关的计划风险来选择合格的安全工程提供商；

(2) 工程组把投资集中在安全工程工具、培训、过程定义、管理实施和改进上;

(3) 基于能力的保证,也就是说,信赖是基于对工程组织安全工程实践和过程成熟的信心。

随着社会对信息信赖程度的增长,信息的保护变得越来越重要。维护和保护信息需要许多产品、系统和服务。安全工程的焦点已经从保护管理政府保密数据转向保护更广泛的应用领域,其中包括金融交易、契约合同、个人信息和因特网(Internet)。这种发展趋势无疑将提高安全工程在未来的重要性。

SSE-CMM 的范围包括下面几项。

(1) SSE-CMM 涉及可信产品或系统整个生命期的安全工程活动,其中包括概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止。

(2) SSE-CMM 可用于安全产品开发者、安全系统开发者、集成商和提供安全服务和安全工程的组织机构。

SSE-CMM 可应用于所有类型和大小的安全工程机构,如商务机构、政府机构和学术机构。

有各类组织从事安全工程,其中包括产品开发者、服务提供者、系统集成者、系统管理者,直至安全专家。其中部分组织处理高层问题(如运行使用或系统体系结构有关的问题),部分组织处理底层问题(如机制选择和设计),还有一部分组织涉及这两个层面。某些组织可能专长于某些特殊技术或某些特殊环境(如在海上)。

SSE-CMM 的设计可用于所有这些组织。采用 SSE-CMM 并不意味着侧重其中某一个方面优于另一个方面,也不意味着 SSE-CMM 所有方面都需要采用。组织的商务侧重点不必由于使用 SSE-CMM,而发生偏离。

根据组织关注的焦点,可采用部分而不是全部的已定义安全工程实施过程。此外,组织可能会需要了解不同实施的关系来确定实施过程的适用性。

本节举例说明了 SSE-CMM 实施活动如何应用于具有不同业务焦点的组织或团体。

SSE-CMM 所定义的元素均认为是安全工程实施的本质要素。但是,并非所有项目或组织需要实施 SSE-CMM 的所有过程区。因此,对于特定项目应该使用裁剪过程以去掉出组织安全工程过程中不必要的过程区。

使用任何参考模型的任何过程改进均应支持商务目标,而不是指导商务目标。使用 SSE-CMM 的组织应根据商务目标来划分过程区实施的优先顺序,并首先致力于改进最高优先级的过程区。

需要注意的是裁剪是在过程区的层面上执行的。为了达到一个过程区的目标,使用把所有的基本实施都放在适当的位置的思想来撰写过程区。

为测量一个组织的从事风险评估的过程能力,会涉及多个实施组共同参与。在系统开发或集成期间,需要评估该组织决定与分析安全脆弱性的能力,并且评估运行的影响。在这种运行情况下,评估组织对系统安全态势监控的能力,识别并分析安全脆弱性,以及评估运行的影响。

在一个组织以开发防范措施为主的情况下,组织的过程能力使用 SSE-CMM 的实施组合来特征化。该模型包含的实施提供了决定和分析安全脆弱性、评估运行影响和为其他组织(如软件组织)提供指南和提供输入。提供开发防范措施的服务组织需要理解上述实施间